09/914315
JC03 Rec'd PCT/PTO 24 AUG 2001

SUBSTITUTE SPECIFICATION

SECURED ACCESS DEVICE WITH CHIP CARD APPLICATIONS

Field of the Invention

The present invention relates to a secured access device for chip card applications. More specifically, the invention relates to a device for secured access to chip card applications that uses instructions that have been performed in the chip card which, at each instant, provide information on rights for accessing the memory of the chip card, the software component, or the hardware operation that has been performed in the chip card.

Background of the Invention

The most common type of chip card has a microprocessor that manages a program memory. The program memory is usually dedicated to a single application or a set of applications loaded at the same time into the chip card. When several applications are loaded into a chip card, they have a close relationship with one another, and are all designed for the same type of service. Thus, for example, a chip card cannot simultaneously play the role of a bank card and that of a customer card for another type of business.

In order to end this situation where each chip card has to be limited to one type of application, new software architectures are being considered. These new software architectures are making use of the development of standardized programming languages which resolve the problems of portability, such as the programming language JAVA, for example.

Figure 1 is a simplified view of a software architecture of the chip cards that are now being developed. The architecture shown in Figure 1 includes, in particular, a first part 110 that corresponds to the software architecture and a second part 120 that corresponds to the applications part of the software architecture for the chip card 100. The system part 110 is essentially formed by a library of programs 112 for the operating system of the chip card, an interface 114 to manage the interactions with the microprocessor or the different memories of the chip card, and a space for the management of hardware interruptions 116.

The applications part 120 of the software architecture includes different applications, such as a first, second and third main application, respectively 122, 124 and 126, and a first, second and third additional application, respectively 121, 123 and 125. The main applications 122, 124 and 126 are written in a programming language that can be directly understood by the processor of the chip card.

The additional applications 121, 123 and 125 are typically applications encoded in a standardized language. These applications may be added at any point in time to the system part 110. In Figure 1, the additional applications 121, 123 and 125 depend directly on the first main application 122. The first main application 122 herein serves as an interpreter

between the additional applications and the operating system by converting the codes of the additional applications into a machine language that can be understood by the programs of the operating system 112.

The software architecture that has just been described is more complex than the one currently existing in chip cards in circulation. The architecture described assumes that it is possible to add applications in a standardized programming language, possibly after the chip card is put into circulation. It is therefore more complicated to achieve a satisfactory level of security compared to when a single application or a group of applications dedicated to a single chip card function are the only applications to be loaded into the chip card. The chip card was then permanently limited in terms of available applications. The risk that a new application might disturb the operation of previous applications was therefore not as great.

The coexistence of applications of different kinds in the same chip card may raise a certain number of problems. For example, a software architecture simultaneously containing an application dedicated to the assessment of a customer's access to a gasoline company and a standard banking application must ensure that a secret key used in the banking application cannot be read during the use of the application associated with the gasoline company.

Summary of the Invention

It is an object of the present invention to overcome the problems that have just been described.

A device is provided that enables the management of different software applications that are installed, possibly at different times, or the